An Enhanced Secure Smart Card-based Password Authentication Scheme

Hsieh-Tsen Pan[1], Hung-Wei Yang[1], and Min-Shiang Hwang[1,2]
(Corresponding author: Min-Shiang Hwang)
Department of Computer Science & Information Engineering, Asia University, Taichung, Taiwan[1]
Department of Medical Research, China Medical University Hospital, China Medical University, Taiwan[2]
(Email: mshwang@asia.edu.tw)
(Received Mar. 3, 2019; Revised and Accepted Dec. 12, 2019; First Online Feb. 28, 2020)

Abstract

The development of world communication and information technology is very advanced. The use of the Internet and smart cards makes it easier for users to conduct remote transactions, and security factors are the key to successful remote users' transactions. In this case, the authentication process is critical to maintaining confidentiality when transactions use public channels. Recently, Moon et al. proposed an efficient and secure smart card based password authentication scheme. They claimed that their scheme is more secure and practical as a remote user authentication scheme. However, Irawan and Hwang found that the Moon et al.'s scheme was still unable to withstand gussing identity attacks and user impersonation attacks. To address this security hole, we propose a new authentication scheme and a key with a smart card in this article. In addition, we show that the proposed authentication scheme is highly resistant to various attacks. Finally, we compare the performance and functionality of the proposed scheme with other related schemes.

Keywords: Password; Smart Card; User Authentication

1 Introduction

Everyone needs security at home, in the office, on the street, and everywhere, because it enables people to use security systems safely and prevent things that shouldn't happen. The safety system should be flexible, cheap, and work continuously without being limited by working hours. With the rapid development of cloud computing, more and more applications and services have been provided, such as cloud storage services, cloud resources, shared computing, and so on [1, 2, 9, 12, 20, 21, 24, 28]. Smart card RFID is an advanced information technology embedded in a card as an information storage medium [8, 25, 26]. At present, the implementation of smart cards has spread to almost all fields, whether it is used in the attendance of hotels, homes, offices and educational institutions, or strict data security.

A user authentication scheme is a mechanism by which a server authenticates users before allowing them to access resources or services provided by the server [14]. To date, many user authentication schemes have been proposed [3, 4, 6, 17, 27]. However, most of these schemes have advantages and disadvantages. In 2012, Yoon et al. proposed a remote user authentication scheme [30], which is an improvement on the scheme of Liaw et al. [19]. However, Chen et al. found that their scheme was not secure enough [7]. In 2012, Li et al. proposed a YS-like user authentication scheme using smart cards [18]. However, Feng et al. found the security of their scheme was vulnerable to the password guessing attack [10]. In 2014, Huang et al. proposed a timestamp-based user authentication with smart card [13]. However, Feng et al. showed that their scheme is vulnerable to the password guessing attack [11]. In 2014, Zhuang et al. proposed a password authentication scheme based on geometric hash function without using smart card [31]. However, Chen showed that their scheme is also vulnerable to the password guessing attack [5].

In 2017, Liu et al. proposed a more secure and practical remote user authentication scheme [22]. However, Moon et al. found that their scheme was still unable to withstand external attacks and offline password guessing attacks [23]. To overcome these security loopholes, Moon et al. also proposed an ECC-based authentication and key agreement scheme using smart cards. Utilizing the lightweight calculation of ECC (Elliptic Curve Cryptography System) [15, 29], Moon et al.'s scheme is both practical and easy to implement. However, in 2018, Irawan and Hwang discovered a security hole in Moon et al.'s two-factor authentication scheme [16]. They showed that Moon et al.'s scheme was actually unable to resist anonymous interception and user impersonation attacks. To overcome these security loopholes, we propose an improved biometric-based authentication and key agreement scheme using smart cards. In addition, we will prove that the proposed authentication scheme is more resistant to

various attacks than other related schemes.

For more details, we divide this article into the following five sections: In Section 1, we briefly introduce our research motivations. In Section 2, we briefly reviewed the weaknesses of Moon et al.'s password authentication scheme. In Section 3, we propose a new authentication scheme. The security and performance analysis of the proposed scheme is given in Section 4, and the conclusions of this paper are given in Section 5.

2 The Weaknesses of Moon et al.'s Scheme

In 2018, Irawan and Hwang found that the Moon et al.'s scheme was unable to withstand gussing identity attacks and user impersonation attacks [16]. In this section, we briefly review the attacks proposed by Irawan and Hwang as follows:

Gussing Identity Attack:

Moon et al.'s scheme [23] did not hide the identity ID of user U_i during the login and authentication phases, User $\rightarrow$ Server: $\{AID_i, D_i, E_i, F_i, T_i\}$, Server $\rightarrow$ User: $\{F_i, G_i, T_s\}$. Attackers can easily guess or steal it from unsecured public channels. The attacker can then check $h(ID_i'||(AID_i \oplus ID_i')||F_i||T_s) \stackrel{?}{=} G_i$.

User Impersonation:

Knowing the user ID_i (guest identity) of the first attack, the attacker will send the user ID_i to the server S through a public channel. During the login phase of Attacker $(ID) \rightarrow$ Server: $\{AID_i, D_i, E_i', F_i', T_i\}$, the server will calculate $F_i' = h(ID_i||h(A_i)||E_i'||T_i)$, it is considered a legitimate user.

3 The Proposed Scheme

In this section, we propose a scheme to improve Moon et al., called a new biometric-based password authentication scheme using smart cards [23]. We modify some procedures during registration, login, and authentication phases. In the improved scheme, there are also two participants, namely the i^{th} user U_i and server S.

3.1 Registration Phase

At the beginning of the improved Moon et al.'s scheme, the server S selects x, E, P, and $h(\cdot)$. Here, x denotes a master secret key stored in S; P denotes a base point of the elliptic curve E; and $h(\cdot)$ denotes a collision-resistant hash function. The user U_i then registers with the server S by the following steps and Figure 1:

Step 1. U_i prints personal biometric information BIO_i on the device sensor. Then, the device sensor scans BIO_i, extracts (R_i, P_i) from $Gen(BIO_i) \rightarrow (R_i, P_i)$, and stores P_i in memory. Here, R_i and P_i denote almost random binary strings and U_i's auxiliary binary strings, respectively. Next, U_i selects identity ID_i and password PW_i, and calculates $RPW_i = h(PW_i||R_i)$. Finally, U_i sends a registration request message $\{ID_i, RPW_i\}$ to S over the secure channel.

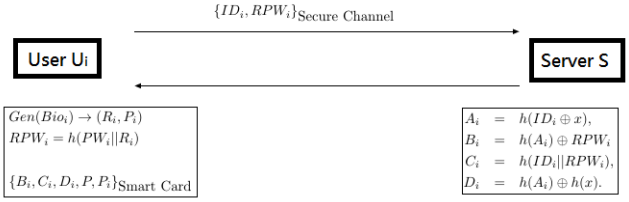

Figure 1: The registration phase of the proposed scheme

Step 2. After receiving the registration request message from U_i, the server S verifies whether ID_i is valid and calculates the following parameters:

$$\begin{aligned} A_i &= h(ID_i \oplus x), \\ B_i &= h(A_i) \oplus RPW_i \\ C_i &= h(ID_i||RPW_i), \\ D_i &= h(A_i) \oplus h(x). \end{aligned}$$

Here, $\oplus$ denotes an exclusive-or operation; and $\|$ denotes a concatenation operation.

Step 3. The server S stores the data $\{B_i, C_i, D_i, h(\cdot), P\}$ on the new smart card, and issues the smart card to the user U_i through a secure channel.

Step 4. The user U_i stores the random number P_i into the smart card.

3.2 Login Phase

After the registration phase is performed, the user will proceed with the login phase to invoke the U_i user to log in to the server S. The steps in this phase are described below and Figure 2.

Step 1. U_i inserts his/her smart card into the card reader, enters ID_i and password PW_i, and then prints biometric information BIO_i^* on the sensor. The sensor then sketches the BIO_i^* and recovers R_i from $Rep(BIO_i^*, P_i) \rightarrow (R_i, BIO_i^*)$.

Step 2. The smart card first calculates two parameters: $RPW_i = h(PW_i||R_i)$ and $C_i' = h(ID_i||RPW_i)$. The smart card then checks if C_i' is equal to the stored C_i. If it is true, the smart card proceeds to Step 3; otherwise, Step 3 is performed. Otherwise, the smart card will terminate this session.

Step 3. The smart card randomly generates a number α

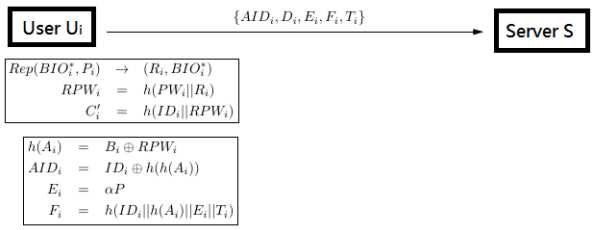

Figure 2: The login phase of the proposed scheme

and calculates the following parameters:

$$\begin{aligned} h(A_i) &= B_i \oplus RPW_i \\ AID_i &= ID_i \oplus h(h(A_i)) \\ E_i &= \alpha P \\ F_i &= h(ID_i||h(A_i)||E_i||T_i), \end{aligned}$$

where T_i is the current timestamp of user U_i.

Step 4. The smart card sends a login request message $\{AID_i, D_i, E_i, F_i, T_i\}$ to the server S.

3.3 Authentication Phase

After completing this phase, the user U_i and the server S can authenticate each other and establish a shared session key for subsequent secret communication. The steps in the certification phase are as follows and Figure 3:

Step 1. The server S verifies $T_i' - T_i \leq \Delta T$, where T_i' is the time to receive the login request message, and ΔT is the valid time threshold. If both conditions are true, the server S proceeds to Step 2; otherwise, the server S proceeds to Step 2. Otherwise, the server S rejects the login request.

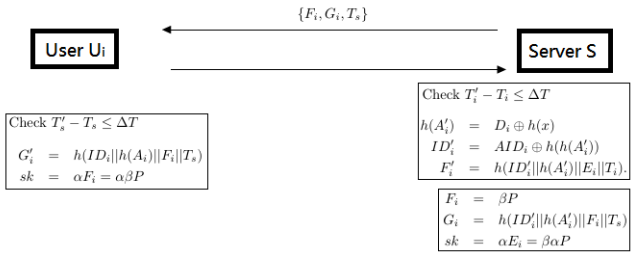

Figure 3: The authentication phase of the proposed scheme

Step 2. The server S calculates the following parameters:

$$\begin{aligned} h(A_i') &= D_i \oplus h(x) \\ ID_i' &= AID_i \oplus h(h(A_i')) \\ F_i' &= h(ID_i'||h(A_i')||E_i||T_i). \end{aligned}$$

The server S then compares whether F_i' is equal to F_i. If it is true, the server S confirms that the user U_i is valid and the login request is accepted; otherwise, the server S confirms that the user U_i is valid. Otherwise, the server S rejects the login request.

Step 3. Next, server S randomly generates a number β and calculates the following parameters: $F_i = \beta P$, $G_i = h(ID_i'||h(A_i')||F_i||T_s)$, where T_s is server S The current timestamp.

Step 4. The server S sends a mutual authentication message $\{F_i, G_i, T_s\}$ to the user U_i.

Step 5. Upon receiving the message $\{F_i, G_i, T_s\}$ from S, the user U_i checks the validity of T_s. If $T_s' - T_s \leq \Delta T$, where T_s' is the time to receive the mutual authentication message, the user U_i proceeds to Step 6; otherwise, the user U_i proceeds to Step 6. Otherwise, the user U_i terminates the connection.

Step 6. The user U_i calculates $G_i' = h(ID_i||h(A_i)||F_i||T_s)$, and then checks whether G_i' is equal to the received G_i. If it is true, the validity of the server S is verified; otherwise, the session is terminated.

Step 7. Finally, the user U_i and the server S construct a shared session key $sk = \alpha\beta P$ to ensure secret communication.

3.4 Password Change Phase

During the password change phase, U_i can update the password without any help from server S. This phase includes the following steps:

Step 1. U_i enters his/her identity ID_i and password PW_i, and print biometric information BIO_i^* on the sensor. The sensor then scans BIO_i^* and recovers R_i from $Rep(BIO_i^*, P_i) \rightarrow R_i$.

Step 2. Next, SC_i calculates $RPW_i = h(PW_i||R_i)$ and checks if $h(ID_i||RPW_i)$ is equal to the stored C_i. If it does, the smart card will ask U_i for the new password; otherwise, SC_i terminates the password change phase immediately.

Step 3. U_i enters a new password PW_i^{new}, smart card further calculates $RPW_i^{new} = h(PW_i^{new}||R_i)$, $B_i^{new} = B_i \oplus RPW_i \oplus RPW_i^{new}$ and $C_i^{new} = C_i \oplus RPW_i \oplus RPW_i^{new}$.

Step 4. Finally, the smart card replaces B_i with B_i^{new} and C_i with C_i^{new} in memory.

4 Security and Performance Analysis of the Proposed Scheme

The improved scheme retains the advantages of the Moon et al.'s scheme [23] and can withstand many types

Table 1: Functionality comparison of the proposed scheme and Moon et al.'s scheme

	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10
Moon et al. [23]	○	○	○	○	○	○	○	○	×	×
The proposed	○	○	○	○	○	○	○	○	○	○

F1: Mutual authentication; F2: Session key agreement; F3: Freely chosen and exchanged password; F4: Withstanding man in the middle attack; F5: Withstanding insider attack; F6: Withstanding replay attack; F7: Providing perfect forward secrecy; F8: Satisfying known-key security; F9: Guessing identity attack; F10: User impersonation attack.

of possible attacks, such as resistance to outsider attacks, insider attacks, user impersonation attacks, and perfect forward secrecy. In this section, we show that the improved scheme can resist gussing identity attacks and user impersonation attacks discovered by Irawan and Hwang [16] and described in Section 2.

4.1 Resisting Gussing Identity Attack

In Moon et al.'s scheme [23], the attacker could intercept $\{AID_i, D_i, E_i, F_i, T_i\}$ in login phase and $\{F_i, G_i, T_s\}$ in authentication phase. The attacker can guess an identity ID_1' and check $h(ID_i'||(AID_i \oplus ID_i')||F_i||T_s) \stackrel{?}{=} G_i$. If the equation holds, the attacker has already guessed the identity ID_i of the user, otherwise, the attacker will repeatedly guess and check other possible identities ID_i'. The main problem is

$$\begin{aligned} G_i &= h(ID_i||h(A_i)||F_i||T_s) \\ &= h(ID_i||(AID_i \oplus ID_i)||F_i||T_s). \end{aligned} \quad (1)$$

Once the attacker knows G_i, AID_i, F_i, and T_s, the attacker can guess ID_i' to satisfy Equation (1).

In the improved scheme, AID_i and ID_i are

$$\begin{aligned} AID_i &= ID_i \oplus h(h(A_i)) \\ h(A_i') &= D_i \oplus h(x) \\ ID_i' &= AID_i \oplus h(h(A_i')). \end{aligned}$$

In the proposed scheme,

$$\begin{aligned} G_i &= h(ID_i||h(A_i)||F_i||T_s) \\ &\neq h(ID_i||(AID_i \oplus ID_i)||F_i||T_s). \end{aligned}$$

It is difficult to obtain $h(A_i)$ from the intercepted $\{AID_i, D_i, E_i, F_i, T_i\}$ during the login phase and $\{F_i, G_i, T_s\}$ during the authentication phase. Thus, the proposed scheme can resist the guessing identity attacks.

4.2 Resisting User Impersonation Attack

In Section 2, we describe that Moon et al.'s scheme cannot resist this guessing identity attack. If the attacker can guess the identity of the legitimate user ID_i, the attacker will impersonate the legitimate user by guessing the identity. In Moon et al.'s scheme, the attacker knows the user ID_i by guessing identity attack, the attacker will impersonate the user ID_i to the server S. During the login phase, the attacker sends $\{AID_i, D_i, E_i', F_i', T_i\}$ to the server. The server will check $F_i' = h(ID_i||h(A_i)||E_i'||T_i)$, so it will be treated as a legitimate user.

Since the proposed scheme can resist identity guessing attacks, the proposed scheme does not have the weakness of the user impersonation attack discovered by Irawan and Hwang [16].

4.3 Performance Analysis

In this section, we compare the functionality between the proposed scheme and the Moon et al.'s scheme in Table 1. If you are interested in comparison with other latest solutions, please refer to [23].

We compare the computational cost between the proposed scheme and the Moon et al.'s scheme in Table 2. If you are interested in comparison with other latest solutions, please refer to [23]. It can be seen from the comparison that the hashing cost of this scheme is slightly higher than that of Moon et al. scheme. Because the coputational cost of ECC operation is much larger than the coputational cost of hash functions and XOR operations. Therefore, we can ignore the computational cost of hash functions and XOR operations. In other words, the computational cost of the proposed scheme is almost equal to that of Moon et al.

5 Conclusion

In this paper, we have proposed an improved Moon et al.'s scheme. We also show that the proposed scheme can against the guessing identity attack and the user impersonation attack.

Acknowledgments

This research was partially supported by the Ministry of Science and Technology, Taiwan (ROC), under contract no.: MOST 108-2410-H-468-023 and MOST 108-2622-8-468-001-TM1.

Table 2: Computational cost comparison of the proposed scheme and other related schemes

	C1	C2	C3	C4	C5	C6	Total
Moon et al. [23]	1H+1F	4H+4X	5H+1F+2P+2X	4H+1F+2P+3X	3H+1F+4X	-	17H+4F+4P+13X
The proposed	1H+1F	5H+3X	6H+1F+2P+2X	5H+1F+2P+2X	3H+1F+4X	-	20H+4F+4P+11X

C1: Computational cost of the user in registration phase; C2: Computational cost of the server in registration phase; C3: Computational cost of the user in login and authentication phases; C4: Computational cost of the server in login and authentication phases; C5: Computational cost of the user in password change phase; C6: Computational cost of the server in password change phase; H: Hashing operation; E: Modulus exponential operation; S: Symmetric encryption/decryption operation; M: Multiplication/division operation; Null: P: ECC operations; X: XOR operations; F: Fuzzy extraction; Null: Cannot provide this functionality.

References

[1] D. S. AbdElminaam, "Improving the security of cloud computing by building new hybrid cryptography algorithms," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 40–48, 2018.

[2] M. H. R. Al-Shaikhly, H. M. El-Bakry, and A. A. Saleh, "Cloud security using Markov chain and genetic algorithm," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 96–106, 2018.

[3] M. Bayat, M. B. Atashgah, M. Barari, and M. R. Aref, "Cryptanalysis and improvement of a user authentication scheme for internet of things using elliptic curve cryptography," *International Journal of Network Security*, vol. 21, no. 6, pp. 897–911, 2019.

[4] S. Q. Cao, Q. Sun, and L. L. Cao, "Security analysis and enhancements of a remote user authentication scheme," *International Journal of Network Security*, vol. 21, no. 4, pp. 661–669, 2019.

[5] S. M. Chen, C. S. Pan, M. S. Hwang, "Cryptanalysis and improvement of Zhuang-Chang-Wang-Zhu password authentication scheme", in *The 2nd Congress on Computer Science and Application (CCSA'14)*, pp. 118–123, 2014.

[6] T. Y. Chen, C. C. Lee, M. S. Hwang, J. K. Jan, "Towards secure and efficient user authentication scheme using smart card for multi-server environments," *Journal of Supercomputing*, vol. 66, no. 2, pp. 1008–1032, Nov. 2013.

[7] T. Y. Chen, C. H. Ling, M. S. Hwang, "Weaknesses of the Yoon-Kim-Yoo remote user authentication scheme using smart cards", in *IEEE Workshop on Electronics, Computer and Applications*, pp. 771–774, 2014.

[8] Y. C. Chen, W. L. Wang, M. S. Hwang, "RFID authentication protocol for anti-counterfeiting and privacy protection", in *The 9th International Conference on Advanced Communication Technology*, pp. 255–259, 2007.

[9] P. S. Chung, C. W. Liu, and M. S. Hwang, "A study of attribute-based proxy re-encryption scheme in cloud environments", *International Journal of Network Security*, vol. 16, no. 1, pp. 1-13, 2014.

[10] T. H. Feng, W. Y. Chao, and M. S. Hwang, "Cryptanalysis and improvement of the Li-Liu-Wu user authentication scheme", in *International Conference on Future Communication Technology and Engineering (FCTE'14)*, pp. 103–106, 2014.

[11] T. H. Feng, C. H. Ling, M. S. Hwang, "An improved timestamp-based user authentication scheme with smart card", in *The 2nd Congress on Computer Science and Application (CCSA'14)*, pp. 111–117, 2014.

[12] W. F. Hsien, C. C. Yang and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133-142, 2016.

[13] H. F. Huang, H. W. Chang, P. K. Yu, "Enhancement of timestamp-based user authentication scheme with smart card," *International Journal of Network Security*, vol. 16, pp. 463–467, 2014.

[14] M. S. Hwang, Li-Hua Li, "A New Remote User Authentication Scheme Using Smart Cards", *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, Feb. 2000.

[15] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of proxy signature based on elliptic curves", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73–84, 2004.

[16] B. Irawan, M. S. Hwang, "The weakness of Moon et al.'s password authentication scheme", in *3rd Annual International Conference on Information System and Artificial Intelligence (ISAI'18)*, Journal of Physics: Conference Series, vol. 1069(1), pp. 012070, 2018.

[17] C. C. Lee, C. H. Liu, M. S. Hwang, "Guessing attacks on strong-password authentication protocol", *International Journal of Network Security*, vol. 15, no. 1, pp. 64–67, 2013.

[18] J. Li, S. Liu, S. Wu, "Cryptanalysis and improvement of a YS-like user authentication scheme", *International Journal of Digital Content Technology and its Applications*, vol. 7, no. 1, pp. 828–836, 2012.

[19] H. T. Liaw, J. F. Lin, and W. C. Wu, "An efficient and complete remote user authentication scheme us-

ing smart cards," *Mathematical and Computer Modelling*, vol. 44, no. 1-2, July 2006.
[20] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing", *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.
[21] L. Liu, Z. Cao, C. Mao, "A note on one outsourcing scheme for big data access control in cloud," *International Journal of Electronics and Information Engineering*, vol. 9, no. 1, pp. 29–35, 2018.
[22] Y. Liu, C. C. Chang and S. C. Chang, "An efficient and secure smart card based password authentication scheme," *International Journal of Network Security*, vol. 19, no. 1, pp. 1–10, 2017.
[23] J. Moon, D. Lee, J. Jung, D. Won, "Improvement of efficient and secure smart card based password authentication scheme," *International Journal of Network Security*, vol. 19, no. 6, pp. 1053-1061, 2017.
[24] S. Rezaei, M. A. Doostari, M. Bayat, "A lightweight and efficient data sharing scheme for cloud computing," *International Journal of Electronics and Information Engineering*, vol. 9, no. 2, pp. 115–131, 2018.
[25] C. H. Wei, M. S. Hwang, A. Y. H. Chin, "A mutual authentication protocol for RFID", *IEEE IT Professional*, vol. 13, no. 2, pp. 20–24, Mar. 2011.
[26] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "A secure privacy and authentication protocol for passive RFID tags," *International Journal of Mobile Communications*, vol. 15, no. 3, pp. 266–277, 2017.
[27] H. Wijayanto, M. S. Hwang, "Improvement on timestamp-based user authentication scheme with smart card lost attack resistance," *International Journal of Network Security*, vol. 17, no. 2, pp. 160–164, 2015.
[28] C. Yang, Q. Chen, Y. Liu, "Fine-grained outsourced data deletion scheme in cloud computing," *International Journal of Electronics and Information Engineering*, vol. 11, no. 2, pp. 81–98, 2019.
[29] C. C. Yang, T. Y. Chang, M. S. Hwang, "A new anonymous conference key distribution system based on the elliptic curve discrete logarithm problem", *Computer Standards and Interfaces*, vol. 25, no. 2, pp. 141-145, 2003.
[30] E. J. Yoon, S. H. Kim, and K. Y. Yoo, "A security enhanced remote user authentication scheme using smart cards," *International Journal of Network Security*, vol. 8, no. 5, pp. 3661–3675, 2012.
[31] X. Zhuang, C.C. Chang, Z.H. Wang, Y. Zhu, "A simple password authentication scheme based on geometric hashing function," *International Journal of Network Security*, vol. 16, pp. 271–277, 2014.

Biography

Hsien-Tsen Pan received B.S. in Business Administration From Soochow University, Taiwan in 1999; M.S. in Information Engineering, Asia University, Taiwan in 2015; Doctoral Program of Information Engineering, Asia University, Taiwan from 2015 till now. From 2011 to 2014, he was the manager in Enterprise Service Chunghwa Telecom South Branch Taichung Taiwan. From 2014 to 2017, he was the operation manager in Medium division Taiwan Ricoh Co., Ltd. Taichung Taiwan From 2017 Sep 20 he is the Apple MDM Server Service VP in Get Technology Co.Ltd. Taipei Taiwan.

Hung-Wei Yang received B.S. in Industry Engineer From Da-Yeh University, Taiwan in 2001; M.S. in Information Management, Chao Yang University, Taiwan in 2009; Doctoral Program of Information Engineering, Asia University, Taiwan from 2016 till now. From 2012 to 2014, he was the manager in International Business Machine. From 2014 to 2015, he was the manager in Cisco Systems, Inc. Taiwan branch. From 2016 to 2019 he is the sales director of China branch in Syntron Technology Co. Ltd. Taipei Taiwan .From 2020 he is channel director in M-Power Co. Ltd., Taipei Taiwan.

Min-Shiang Hwang received M.S. in industrial engineering from National Tsing Hua University, Taiwan in 1988; and Ph.D. degree in computer and information science from National Chiao Tung University, Taiwan in 1995. He was a professor and Chairman of the Department of Management Information Systems, NCHU, during 2003-2009. He was also a visiting professor with University of California (UC), Riverside and UC. Davis (USA) during 2009-2010. He was a distinguished professor of Department of Management Information Systems, NCHU, during 2007-2011. He obtained the 1997, 1998, 1999, 2000, and 2001 Exceilent Research Award of National Science Council (Taiwan). Dr. Hwang was a dean of College of Computer Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor with Department of Computer Science and Information Engineering, AU. His current research interests include information security, electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 300+ articles on the above research fields in international journals.